NAVAL WAR COLLEGE
Newport, RI

Submarines and Information Operations

Charles A. Richard
CDR, USN

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of Elective Course WE-519, Information Operations.

Signature: CDR USN

8 May 2000

UNCLASSIFIED
Security Classification This Page

REPORT DOCUMENTATION PAGE

1. Report Security Classification: UNCLASSIFIED	
2. Security Classification Authority:	
3. Declassification/Downgrading Schedule:	
4. Distribution/Availability of Report: DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.	
5. Name of Performing Organization: Dean of Academics Office	
6. Office Symbol: 1	7. Address: NAVAL WAR COLLEGE 686 CUSHING ROAD NEWPORT, RI 02841-1207
8. Title (Include Security Classification): Submarines and Information Operations (U)	
9. Personal Authors: Charles A. Richard, CDR, USN	
10. Type of Report: FINAL	11. Date of Report: 8 May 2000
12. Page Count: 20	
13. Supplementary Notation: A paper submitted to the Dean of Academics, Naval War College, for the Naval Submarine League essay competition. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.	
14. Ten key words that relate to your paper: Submarine, Information Operations, Information Warfare, SSN, UAV, UUV, Electronic Warfare, Operational Security, Information Assurance.	

15. Abstract:

Information Operations and Information Warfare are efforts to exploit a resource that has long been essential for military operations: information. Information has become a new medium for conflict, a potent weapon, and a lucrative target. The manned, mobile, combatant platform can conduct Information Operations. The nuclear-powered attack submarine, and its inherent virtues of stealth, mobility, endurance, and power-density, gives unique opportunities for employment. As the U.S. Navy intends to embed IO capabilities in the fleet, sailors, not scholars, need to begin to examine and exploit the field.

16. Distribution / Availability of Abstract:	Unclassified	Same As Rpt	DTIC Users
	X		

17. Abstract Security Classification: UNCLASSIFIED	
18. Name of Responsible Individual: Dean of Academics, Naval War College	
19. Telephone: 841-2245	20. Office Symbol: 1

Security Classification of This Page: UNCLASSIFIED

Encl (2)

Abstract of

Submarines and Information Operations

Information Operations and Information Warfare are efforts to exploit a resource that has long been essential for military operations: information. Information has become a new medium for conflict, a potent weapon, and a lucrative target. The manned, mobile, combatant platform can conduct Information Operations. The nuclear-powered attack submarine, and its inherent virtues of stealth, mobility, endurance, and power-density, gives unique opportunities for employment. As the U.S. Navy intends to embed IO capabilities in the fleet, sailors, not scholars, need to begin to examine and exploit the field.

Offensive information operations require access to adversary information, and often benefit if the operations are not detected. While global networks such as the Internet will allow some degree of access, manned mobile platforms will be required for access in some situations. Submarines have a unique combination of stealth, endurance, mobility, and energy at their disposal. They offer a unique degree of access to information. This access can be obtained from sensors onboard the ship, from unmanned vehicles launched from the sub, or from manned special operations originating from sea. This access can be used to obtain otherwise unobtainable information, or as a crosscheck on data from other assets. For defensive operations, the submarine is difficult to target, and resistant to directed energy weapons.

Future visions of the battlefield predict the sophisticated platform giving way to numerous simple sensors and weapons. As we make this transition, the manned platform will be needed to both "spin the web" and act as its first node until communications and deployment technology advance to the point where this is no longer required. The submarine will be an ideal candidate for this mission.

Submarines, like all platforms, have limitations. For example, submarines trade electromagnetic spectrum access, for both communications and sensing, with stealth and speed. Some missions will be better assigned to other platforms with their virtues.

Submarines today offer unique capabilities to a Navy or Joint IO campaign. New technologies offer the promise of greatly expanding that capability. The Fleet and her sailors should begin to take information operations out of the classroom, test it, and put it to work in the real world.

Introduction

Information Operations and Information Warfare are new efforts to understand and exploit a resource that has long been essential for successful national defense and military operations: information. The U. S. military is increasingly attempting to capitalize on the growing sophistication, connectivity, and reliance on information technology.[1] The information realm has become a new area of combat, with some similarities to the manner in which aerospace became a medium of conflict in the early 20th century. It is one component in a technology-driven Revolution-in-Military Affairs that could potentially reshape completely the manner in which conflicts are contested and resolved.

This paper examines potential roles and missions for a manned, mobile, combatant platform in conducting Information Operations and Information Warfare. Specific attention is focused on nuclear-powered attack submarines, and their inherent virtues of stealth, mobility, endurance, and power-density. Some of this discussion will be applicable to other platforms as well. Although this paper focuses on submarines, this is not to imply that other Navy assets have no role in Information Operations. Quite the contrary, every fleet element has a unique combination of strengths and weaknesses when considered for potential assignments in an IO campaign. Each should be examined in this light as a first step towards planning employment. This paper's focus on submarines is done only to limit the scope of the discussion for this paper.

Background

Information Operations (IO) involve actions taken to affect adversary information and information systems while defending one's own information and information systems.[2] Information Operations is a broader term than Information Warfare (IW), includes IW, and extends the concept to operations conducted in times other than war. The distinction between IO and IW is relatively new, and many references referring to IW can also be applied to IO. Information Operations have both an offensive and defensive component, and it already has doctrine in place to guide its execution in the joint warfighting process.

The Navy intends to have "a prominent role" in Information Operations and Information Warfare, and to "embed IW capabilities in the fleet."[3] Yet, due to the recentness of IO as an encompassing field of study, many of the available references tend to be of an academic nature, and tend to be more theoretical than practical in their treatment of the subject. The "operators", the men and women who apply these

concepts in real-world operations to achieve practical results, have written little. To begin examining potential roles and missions for manned mobile platforms, particularly the submarine, in an Information Operations campaign, it is helpful to examine Information Operations, split it into its core components, and examine possible mechanisms by which it can have effect.

Offensive Information Operations targets the human decision making process.[4] It is utilized at all levels of war (Strategic, Operational, and Tactical). It may have the greatest impact on adversary decision-makers in peacetime, or in the initial stages of a crisis.[5] Its assigned and supporting capabilities can include:

Electronic Warfare	Psychological Operations (PSYOPS)
Physical Attack/Destruction	Operational Security (OPSEC)
Computer Network Attack (CNA)	Military Deception

Table 1.

Offensive Information Operations Capabilities

The vulnerabilities that exist in potential adversaries that give rise to the possibility for Offensive Information Operations also exist for U.S. forces, and gives rise to Defensive Information Operations, to protect friendly information from the actions of an adversary. "Defensive Operations ensure timely, accurate, and relevant information access while denying adversaries the opportunity to exploit friendly information and information systems for their own purposes."[6] Defensive Information Operations can include:

Information Assurance (IA)	Information Security (INFOSEC)
Physical Security	Operational Security (OPSEC)
Counterdeception (CD)	Counterpropoganda
Counterinformation (CI)	Electronic Warfare

Table 2.

Defensive Information Operations Capabilities

In examining potential submarine IO assignments, it is also useful to draw another distinction, that between Information Warfare and Information Age Warfare. Information age warfare uses information technology as a tool to impart combat operations with unprecedented economies of time and force.[7] In contrast, information warfare views information itself as a separate realm, potent weapon, and lucrative target.[8] This paper focuses on the latter.

<u>Discussion</u>

One theory of information warfare breaks offensive information warfare into three types of operations: increased availability of information to the player on the offensive, decreased availability of information to the player on the defensive, and decreased integrity of the information itself.[9] It can been seen that the above listed (Table 1) assigned capabilities for offensive information operations can each be accomplished by some combination of these three actions.

In order to accomplish any of the three, the offensive player must first establish access to the information (in order to increase its availability to him, or to tamper with its integrity), or at least establish access to the system used to communicate or manipulate that information (in order to decrease its availability to the defensive player). While it is popular to think of "cyberwar" as being conducted by a new cadre of "information warriors" sitting at computer consoles somewhere in the heartland of America, winning the United State's conflicts via the intercommunications provided by the Internet, this will not always be the case.[10] Not all systems are interconnected to the Internet; in fact most militarily valuable systems are *not* connected to the Internet. Often, the access required to conduct Information Operations

will require a manned mobile platform to move into position to provide this access. Often, the best platform will be the nuclear powered submarine.

The ability to avoid detection is of great advantage in conducting Offensive IO. Deming notes "If tampering goes undetected, the effect can be worse than that of total destruction, as the corrupted data might be used in ways that undermine the objectives of the defense."[11] Similarly, both indications and warning and detection are considered important aims of the defense. Stealth, then, is of great advantage to the attacker in information operations. Stealth minimizes the indications that tampering has occurred, and reduces the opportunities the defense has to detect that data has been corrupted. Nuclear powered submarines combine stealth with access.[12]

Submarines have considerable endurance at their disposal. They can remain on station for months and do not rely on forward bases, logistic trains, or pre-positioned supplies. The freedom to operate anywhere in world without the need for resupply and logistic support reduces the demands on the theater commander and is a major advantage of the submarine.[13] Since Information Operations are conducted in peacetime as well as crisis and war, this endurance gives the battle group or Joint Task Force commander considerable flexibility. This endurance enables sustained Information Operations that can serve as a deterrent, provide situational awareness, prepare the battlefield for future operations if necessary, and support contingency operations.[14]

Nuclear power also provides significant power density, power endurance, and frees the ship from the need to refuel. As will be discussed later, this will become of increasing advantage as new generations of power intensive directed energy weapons become available.[15]

Offensive IO: Electronic Warfare

Electronic Warfare (EW) is any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or attack the enemy. Submarines have long been involved in intelligence gathering and surveillance, and often utilize the electromagnetic spectrum to accomplish this.[16] Utilizing their stealth, mobility, and endurance, a submarine may provide the only access to the electromagnetic spectrum in an important area. This access will grow in importance in the future. The worldwide wireless industry has seen a large increase in the demand for wireless services, and this demand is expected to continue to increase substantially.[17] Some countries are establishing nearly completely

wireless communications infrastructures.[18] This increasing utilization of wireless technologies could be successfully exploited given access to the spectrum. These newer wireless technologies utilize more sophisticated signal processing techniques, shorter-range links to network nodes, advanced capability antennas, and lower power levels. These steps are done to improve the efficiency and quality of service to the users, but a secondary effect is to make traditional Signals Intelligence (SIGINT) systems less effective. For many new systems, the access afforded by a submarine, and the resulting short-range, line-of-sight path that it provides may be the only avenue available for SIGINT exploitation.

Passive RF monitoring need not be limited to traditional SIGINT targets. Once a sub is in position to conduct traditional SIGINT, it is a simple manner to expand this to full spectrum exploitation, including open source and broadcast medium monitoring. Although similar information may be available from other sources, the fusion of this data onboard the forward-deployed platform may show correlation that might otherwise be missed. Additionally, the availability of tactical communications links to the Battle Group or Joint Task Force Commander may be able to get important information to the JTF IO Planning Cell faster than other methods requiring reachback to CONUS.

The submarine participation need not be limited to simple passive monitoring of the Radio Frequency (RF) spectrum. Several new offensive technologies are emerging, including High Power Microwave (HPM) and High-Energy Radio Frequency (HERF) guns. The concept behind such weapons is to generate an electromagnetic wave of sufficient magnitude to damage the adversary's electronics.[19] While such weapons are several generations away from having useable ranges suitable for fleet use, submarines make good candidates as deployment platforms. In addition to being able to provide access in many situations for their use, submarines have the physical space necessary to carry such weapons. The nuclear power source of these ships not only has the power supply capacity to supply the energy necessary for this type of weapon, there are new initiatives on the horizon to make further power available for directed energy systems. One example is all electric propulsion, recently announced as a possible choice for the DDG-21 series of ships.[20] By making all power generation onboard ship electric, power can be diverted between propulsion and weapons systems with a much greater degree of flexibility than exists today. All electric drive for submarines would provide similar advantages.

Directed energy weapons are not restricted to the RF portions of the spectrum. Considerable work has been done with optical systems as well. Laser systems offer the potential to "dazzle" satellite sensors, temporarily or permanently blinding them. They can also effect the physical destruction of objects including satellites.[21] Their shorter wavelength allows for much tighter focusing and narrower beamwidths than RF systems. The advantages of submarine deployment of such systems not only include the mobility and stealth afforded by a boat, but other advantages as well. Some target satellites, particularly ones in a geosynchnrous or geostationary orbit, might not be accessible from land-based stations under friendly control. Ship platforms could carry and support higher power and physically larger equipment than airborne equipment. Also, the submarine force has considerable experience from the SSBN community in obtaining the platform stability and position accuracy that such a system may require to accurately and reliably hit only the desired target. Such optical systems are likely to be expensive and few in number, at least initially, and the submarine force has a proven track record in providing a high degree of survivability to high value weapons systems, such as strategic missiles.[22]

As directed energy weapons become more feasible, and begin to be deployed, the power and propulsion systems on the platforms they are installed on take on a new significance. The power system becomes, in effect, the platform's "weapons magazine" in addition to its propulsion source. Instead of counting available bombs, missiles, or gun rounds, the number of available megawatt-hours of power without refueling will be the metric. Nuclear power will become an even more important advantage, providing up to 4 orders of magnitude improvement over chemically fueled platforms in available power for both weapons and propulsion.

Submarines need not be limited to their installed masts and antennas for Electronic Warfare. The use of Unmanned Aerial Vehicles (UAVs) launched from submarines has been shown to be feasible.[23] Recently, USS Chicago (SSN 721) was fitted with the Predator UAV Command, Control, Communications and Intelligence (C3I) system. Using Ultra High Frequency (UHF) Satellite Communications, the USS Chicago was able to operate and maneuver the Predator UAV demonstrating the ability to sense over 100 miles into the enemy's back yard. USS Chicago successfully demonstrated the ability to:

- Conduct tactical reconnaissance on a land-based mobile missile battery
- Fusing UAV imagery and sensor data and relaying this information to the Joint Task Force Commander
- Selecting Special Forces (SOF) mission ingress / egress routes
- Monitoring mobile missile movements in support of SOF strike mission.

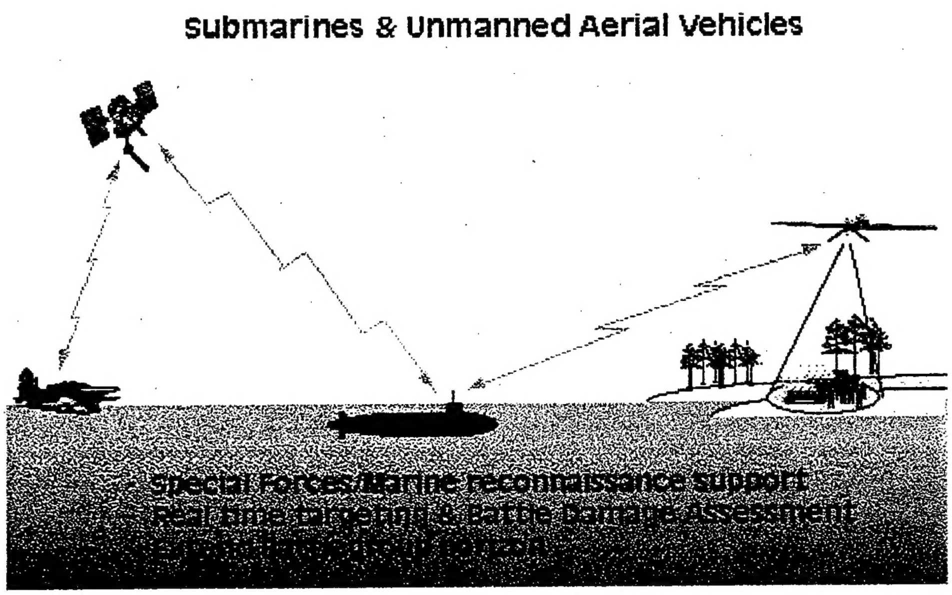

Figure 1

Submarine Launched UAV[23]

All of this could be conducted in areas inaccessible to other elements of the Joint Task Force. The submarine need not directly control the unmanned vehicle. Once deployed, the UAV could be controlled via a satellite link from any element in the Battle Group, or conceivably from CONUS. The submarine could simply be the deployment and recovery platform, or the UAV could be designed for a one way mission.

UAV technology is advancing at a very rapid rate. Feasible capabilities in the near future range from "Upper Tier" craft, very high altitude, high-endurance vehicles that can be thought of as tactically employed, near geostationary, low-earth orbiting satellites. The other extreme described was the "Lower Tier" craft, envisioned as 10-15 foot wingspan vehicles carrying approximately 100 pounds of payload.[24] UAVs of this size are feasible for submerged launch from a submarine, either from a torpedo tube, or from

a future ocean systems interface. The technology for this type of UAV is available now. Recently, the Aerosonde UAV, a 30 pound vehicle carrying 1.5 gallons of gasoline, made a 2030 mile transatlantic crossing. It carried communications, navigation, and meteorological sensing equipment, and the total cost of the craft was $25,000.[25] Equipped with small, low radar cross section UAV such as this, a submarine can place them into positions unreachable by any other element of the JTF, obtaining valuable information and acting as an enabler for follow-on forces.

Acoustic Warfare

Similar to the use of electronic methods to achieve battlespace awareness on or above the surface of the water, acoustic methods are among those used to achieve Undersea Battlespace awareness. In much the same way as Electronic Warfare is conducted, as discussed above, it is also possible to conduct Acoustic Warfare in the Undersea Environment. A submarine is in an ideal position to contribute significantly to the development of Undersea Battlespace awareness, and also to ascertain and influence an adversaries attempt to do the same. Other sensors, such as aircraft and satellites, are severely constrained on their ability to determine the underwater picture.

Submarines are not limited to organic sensors in their ability to sense and influence the underwater battlespace. Unmanned Undersea Vehicles (UUVs) and Autonomous Undersea Vehicles (AUVs) will provide many of the same advantages underwater that UAVs offered for aerial operations. The Naval Undersea Warfare Center is developing three experimental UUVs with ranges up to 30 miles and a variety of sensor packages.[26] Such systems would be useful in mine reconnaissance and anti-submarine warfare, as well as surveillance prior to an amphibious assault. In addition to providing expanded awareness of the undersea battlefield, UUVs and AUVs offer promise to improve communications connectivity with submerged submarines without restricting their maneuverability and operating envelope. For example, the Naval Ocean Systems Center (NOSC) San Diego "Flying Plug" concept would provide a submerged submarine with fiber-optic connectivity while maintaining full maneuverability over a large (20 km) area while communicating with either surface forces, or to fixed undersea array systems.[27] Naval Undersea Warfare Center (NUWC) Newport is working on the SmartComm system, which is designed to allow high data rate communications to a submerged submarine over a wide operating envelope. The system is envisioned to provide communications to torpedoes and surface ships, as well as undersea sensor networks.

Target data rate is 30 Mbits/sec full duplex, well in excess of any system currently available to submarines today, and approximately 20 times that of a T1 line.[28]

Computer Network Attack

"The process of breaking into a computer generally involves getting access to an account on the system."[29] Although this is typically thought of in terms of remote access, perhaps via the Internet, this is not always the case. Some systems are not attached to the Internet. However, there may be other vulnerabilities that can be exploited.

A large portion of international communications, both data and voice, moves not on satellites, but on underwater cables, and this proportion is expected to increase. The United States' transoceanic cable capacity has increased by a factor of 30 in the last 4 years, and is now approaching 1,000 Gigabits/sec, the equivalent of 70 million simultaneous phone calls.[30] Ultimately, more international bandwidth will be provided by underwater cables than by satellites.

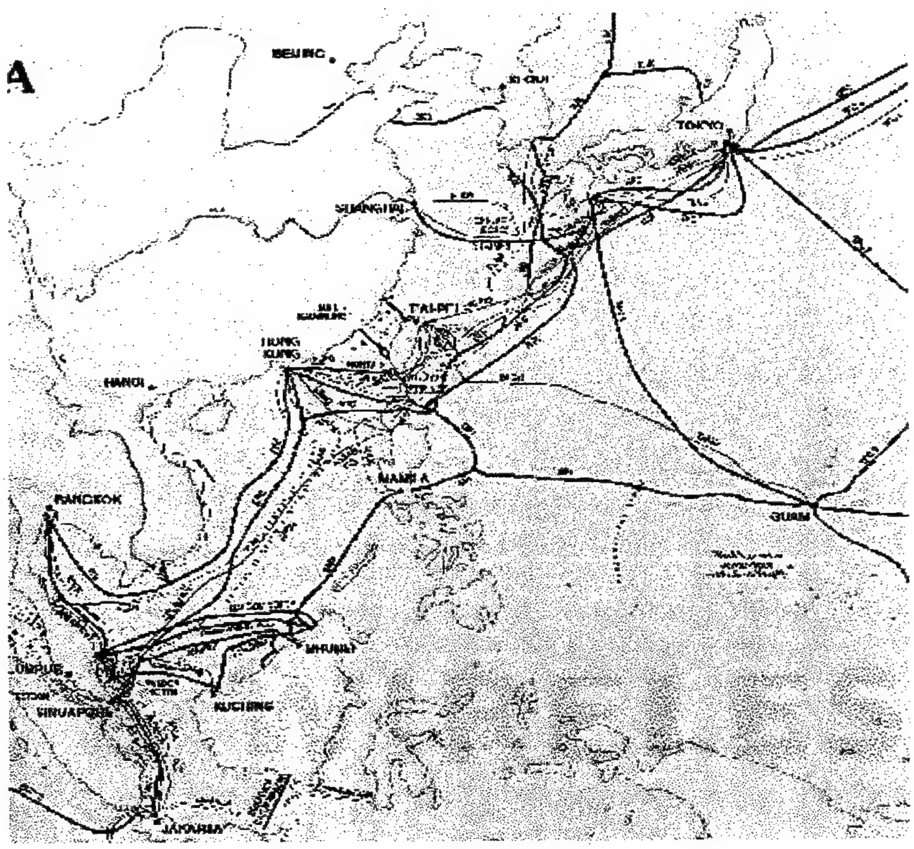

Figure 2

Pacific Rim Undersea Communications Cables

The presence of these cables can be exploited by a variety of means. Use of the submarine allows direct physical access with a high degree of covertness, such that the chance that the adversary is aware of the exploitation is minimal. Figure 2 shows a map of existing submarine cables along the Asian-Pacific Rim.[31]

Other systems may not have any possibilities for attack without directly putting a man "on the ground" to accomplish the desired effect. This may require a Special Forces operation. Submarines have operated with the Special Forces for over 50 years.[32] The submarine provides an ideal platform for the clandestine insertion and extraction of a small team of combat swimmers or Special Operation Forces to conduct a Computer Network Attack (CNA). The endurance of the sub enables such a team to be pre-positioned for long periods of time, on standby for service should a situation deteriorate or otherwise require action. The submarine itself offers the possibility of conducting battle damage assessments, a difficult task in many kinds of CNA, in near real time. The ship could use its onboard sensors to determine the effect of the Special Forces mission and report the results to the Battle Group or JTF.

Physical Attack/Destruction

Submarines, like most combatant vessels in a battle group, carry significant firepower, which is available to conduct physical attack and destruction of targets identified by the JTF IO Cell, as well as by more traditional means. Probably the most useful weapon for this role is the Tomahawk cruise missile. Extended range versions, with Global Positioning System (GPS) guidance, are available now, and even more capable versions are under development.[33] Advanced capability torpedoes and mines are also available.

Military Deception

Military Deception operations are undertaken to mislead adversary decision makers as to friendly capabilities, intentions and operations, causing the adversary to take specific actions that will contribute to the accomplishment of the friendly mission.[34] Military Deception is an involved process. One portion where the stealth and mobility of the nuclear powered submarine can be used to advantage in this process is to be used as the means to deliver the deception. Stealth and mobility provide a high degree of Operational Security (OPSEC) in the delivery of the deception. This delivery mechanism focuses on raising the visibility to the adversary of selected intelligence indicators, in an effort to induce the adversary to take desired actions. As a submarine has virtually no indicators in its own right, it minimizes the risk that the

adversary will detect the deception while it is being delivered. Deception can be used in conjunction with other elements of offensive information warfare. A submarine might provide a series of deceptive electronic emissions intended to cause an adversary to believe a large surface force was located in a given area. Other indicators could be used. For example, a submarine launched Tomahawk strike might be used to initiate a feint during the opening stages of a larger strike mission, causing a reorientation of adversary air defense systems, which could then be exploited by other platforms. The high mobility of the submarine enables it to move into a desired position to deliver the deceptive indicator quickly, then be ready to assume additional tasking once the deceptive mission is complete.

OPSEC and PSYOPS

Submarines have the ability to exercise the same discipline as all other fleet units in denying the adversary critical information about friendly capabilities and intentions. Additionally, the stealth associated with submarine operations is in itself a form of OPSEC, as it denies an adversary locating data that can be used in combination with other information to derive friendly intentions. The access afforded by a boat could be used to determine the effectiveness of a Psychological Operation (PSYOP) attack by monitoring reaction to friendly efforts.

Defensive IO

Many of the same attributes that make a submarine an ideal candidate for assignment for offensive IO tasking also contributes to its defensive IO capability. Submarines have the same abilities as all fleet units to engage in information assurance, information security, operational security and physical security, capabilities included in Defensive IO as shown in Table 2.

The stealth afforded by a submarine adds to the quality and reliability of the information it obtains. Unlike some other assets, e.g. space assets whose positions and orbits may be known by the adversary, the uncertain nature of the location of a boat makes it far more difficult for an adversary to target it in his offensive information plan. It also makes it more difficult for an adversary to take defensive measures against the sensor (e.g. placing objects underground or in buildings to avoid space-based observation). This uncertainty as to the presence of a submarine makes it more likely that intelligence can be obtained on adversary offensive information operations, which in turn enables friendly efforts to counter them.

The data obtained by a submarine may serve as a useful "cross-check" on the reliability of the same information obtained by other friendly sources. This defensive information operation capability serves to enhance and confirm the quality of the intelligence information obtained by other means. While the quantity of information obtained from the submarine may not equal that from, for example, an overhead sensor, it would have a high degree of quality or information assurance. This information assurance is achieved by the submarine's stealth, which makes it unlikely that an adversary would be aware of the presence of the boat or the collection effort. This could provide a means to detect an adversary attempt to insert disinformation or fool an air or space based sensor whose location is predictable and known to the adversary.

The opacity of water to electromagnetic radiation also serves as a defensive mechanism for submarines. An adversary's use of directed energy weapons systems, such as HPM or HERF, would be much less effective against a submarine. Electronic Warfare assets onboard a submarine could serve as a reserve or hardened backup for the Joint Force Commander when faced by the possibility of attack by these types of weapons.

The access to the ocean floor, and the fiber optic communications cables that run across it, provided by submarines can also be used defensively. The United States, as noted before, is increasingly utilizing and dependent upon these types of communications links. Although there are several mechanisms to detect tampering, some of them, such as inspecting the lines with sensors towed from surface ships, are observable by adversaries. Only the submarine offers the covert ability to physically detect intrusion. This attribute can be turned to an offensive opportunity. If a breach is detected covertly, it becomes an avenue to conduct counter-information operations.

Limitations

Submarines, like all platforms, have limitations. Submarines today trade access to the electromagnetic spectrum, for both communications and sensing, with speed and stealth. Mast exposure for antennas and periscopes increase the possibility of detection, and can place limitations on ship's speed. This might limit the number of potential missions a submarine could be assigned. Submarines may best be employed in areas that no other platform can get to. In more permissive environments, the greater height of eye and physical space available for antennas may make a surface ship the preferred platform. For other

occasions where the lack of endurance can be tolerated, the speed and altitude afforded by an aircraft will be preferred. However, new technologies are emerging that can potentially minimize this access-stealth trade-off for submarines. Higher data rate communications systems minimize the time required to exchange information. New solutions, not requiring masts for spectrum access, greatly improve the available operating envelope of speed and depth available to the boat. Network Centric Warfare concepts have the potential to more efficiently use the available submarine bandwidth. Submarines today have sufficient communications capability to conduct Information Operations, and this capability should improve in the future.

The Future

It gets increasingly difficult to predict how warfare will evolve as the time frame for the prediction gets longer. The Navy is currently in transition from a fully platform centric model to a more distributed network centric approach. Chief of Naval Operations Admiral Jay Johnson has called it "a fundamental shift from what we call platform-centric warfare to something we call network-centric warfare, and it will prove to be the most important RMA [Revolution in Military Affairs] in the past 200 years."[35] Some have speculated this transition will continue even further. Martin Libici, senior fellow at the National Defense University, states "Today, platforms rule the battlefield. In time, however, the large, the complex, and the few will have to yield to the small and the many."[36] What he foresees is a battlefield that is covered by systems composed of millions of sensors, micro-projectiles, and other small, highly intelligent objects with the ability to detect, target and destroy any military device desired.[37] Some of the first steps towards this transition are already occurring. Cruise and Ballistic missiles were beginning efforts as man distanced himself from the battlefield while at the same time expanding it. Network Centric Warfare, Unmanned Aerial Vehicles and Autonomous Undersea Vehicles, improved sensor technology and other efforts will continue this trend in the near term. The end state prediction offered by Libicki could very well wind up being true.

However, if so, the nation's military still has to get from here to there. It will still be necessary to go from the platform centric model of today to the mesh and the net envisioned in the future. The first step, integrating and networking all the sensors, weapons, and other capabilities of existing platforms into a composite force, is well underway. This is a part of Network Centric Warfare. As stated by Alberts,

Garstka, and Stein, "NCW [Network Centric Warfare] translates information superiority into combat power by effectively linking knowledgeable entities in the battlespace."[38] The next step, the development of small, unmanned, and remotely operated sensor packages, has started. However, before it would be possible to go all the way to "fire-ant warfare, a battlefield dominated by scads of sensors, emitters, and microprojectiles." a number of significant technical challenges will have to be overcome.[39]

One of the most significant will be the communications links necessary to put this distributed net or mesh together. Bandwidth and range in a communications system requires power, and more power requires more size and cost. It is interesting to note that the development of networked combat technologies and data exchange systems has progressed more quickly in the Navy than it has in the ground services. There may be many reasons for this, but part of it stems from the number of and capabilities present in the platforms on a maritime battlespace compared to those present on a land battlespace. In general, there are fewer platforms present on the maritime battlespace, each one can sense a much larger area than its land counterpart, the ships have significantly greater power capability, and more room for equipment and antennas to interconnect with. The net result is there are fewer pieces to the sea puzzle to be put together, and the resources to do it with are easier to obtain. The mesh described above will have to overcome the same limitations that have made networking the land battlefield more difficult. Mobile power supplies, antenna space and configuration, radio frequency management issues, and security of communications are just a few of the difficult problems involved in building a "mesh" containing thousands or millions of nodes. These issues will be overcome, and it may be possible in the future to engage in "fire-ant warfare" or its equivalent anywhere in the world necessary without having personnel leave the United States. However, it is almost equally certain that the initial implementation of these systems will not have these capabilities. Libici's own example of the use of a sonobouy field as a primitive example of his concept is illustrative.[40] A well placed sonobouy field with high performance sensors is indeed a formidable Anti-Submarine barrier...but today it still requires a manned, mobile platform to obtain the information the sonobouy field senses and then utilize it. Future sensors will undoubtedly have more capability, endurance, smaller size, and communications robustness; but the ability to operate a sonobouy field completely from the beach is still a long way off. The manned, mobile platform is still very much required as a part of the system for the immediate future.

Related to the need to power the mesh, and communicate between its nodes, is the need to deploy it in the first place. Returning to the sonobouy example above, assume that advances in power systems and communications technology have reached the point that a field located anywhere in the world could be operated remotely from CONUS. Given that it is possible to operate the field remotely, it is still unlikely that sufficient sensors could be permanently deployed to continuously monitor all of the world's oceans. The sonobouy system would still require some deployment mechanism, some means to get the mesh installed in the first place. Perhaps this, too will be overcome at some point in the distant future, but until then, it is reasonable to assume that a manned, mobile platform will be required to deploy the sensors that form the mesh.

It seems logical that as the few and the complex transition to the small and the many, this will initially occur by using manned, mobile platforms to "sow" the battlefield then stand-off to monitor and employ the Local Area Combat Net as necessary. Eventually the monitoring and employment function might be accomplished from CONUS without the need for a manned platform to remain in the vicinity to operate the network after deployment. In either case, however, such a standoff or deployment platform would benefit from stealth, mobility, endurance, and access. In many cases, the platform of choice will be the submarine.

Another possibility is that a distributed weapons/sensor net is simply an incorrect prediction as to the shape of future warfare. Although many indications point to the logic of the distributed net conclusion, predicting future trends in warfare has proven to be difficult. The extensive and robust communications necessary for any of the networked or distributed forms of combat force organization could become vulnerabilities that a skilled adversary could exploit. There are similarities between the communications links today and the railroads of the mid-19th century. The Prussians were the first to realize the military advantages in mobility and potential to mass forces provided by the railroads. They used the railroads to considerable advantage in their victory in the Franco-Prussian War.[41] However, countries that exploited the mobility of the railroad to gain combat advantage over their adversaries also exposed new vulnerabilities. In the Chinese Civil War, Chiang Kai-shek overextended his Nationalist forces into Manchuria down long and tenuous rail lines of communications. He was unable to protect this vulnerability, and the Communist

Chinese were able to cut the rail lines off. The Nationalist forces were isolated, and cut off from logistics support, enabling the Communists to defeat them.[42]

In the same manner, the information age presents us with a great opportunity to exploit information along communications links to obtain military advantage over our potential adversaries. This is the core concept in Network Centric Warfare. However, a vulnerability is exposed by the communications links. It is necessary to be prepared to continue to wage war if a skillful adversary denies these links. The stealth, endurance, firepower, mobility and survivability of the submarine gives it the ability to apply more traditional expressions of military force with great vigor, and as such act as a type of "insurance policy" as our forces enter the new realm of the information age and information warfare.

Conclusions

Submarines have been shown to have a unique combination of stealth, mobility, endurance, and power-density that gives these ships a high degree of access to information. This access, in many cases, can not be obtained by other means. This access opens the possibility of a wide range of Information Operations (IO), a new medium of conflict that is just beginning to be examined by the U.S. military. As a new field, Information Operations requires examination by the fleet as to its usefulness in accomplishing the missions assigned to the Navy. U.S. Navy ships and other platforms can participate, without modification, in an IO campaign, which is a stated goal of the Navy. Submarines can today play a key role in these operations, and new technologies offer the promise of greatly expanded capability for both the fleet in general and submarines in particular. The Fleet and her sailors should begin to take information operations out of the classroom, test it, and put it to work in the real world, and submarines can play a key part in this.

Notes:

[1]Joint Chiefs of Staff, Joint Doctrine for Information Operations (Joint Pub 3-13) (Washington, D.C.: October 9, 1998), vii.

[2]Ibid.

[3]Navy Department, Copernicus…Forward. (Washington, D.C.: June 1995).

[4]Joint Chiefs of Staff, Joint Doctrine for Information Operations (Joint Pub 3-13), II-1.

[5]Ibid., viii.

[6]Ibid.

[7]Department of the Air Force, Cornerstones of Information Warfare. (Washington, D.C.).

[8]Ibid.

[9]Dorothy E. Denning, Information Warfare and Security. (Reading, MA: Addison-Wesley 1999), 30.

[10]"Onward Cyber Soldiers" Time Magazine, Vol. 146 Nbr 8, 21 August 1995, 1.

[11]Denning, 35.

[12]"Submarine Capabilities", Submarine Warfare Division (CNO N87) Homepage, <http://www.chinfo.navy.mil/navpalib/cno/n87/capable.html> (Jan 2000).

[13]Ibid.

[14]Joint Chiefs of Staff, Joint Doctrine for Information Operations (Joint Pub 3-13), II-2.

[15]"Submarine Capabilities", Submarine Warfare Division (CNO N87) Homepage

[16]"Submarine Roles and Missions", Commander, Submarine Force Atlantic Fleet (COMSUBLANT) Homepage, < http://www.chips.navy.mil/sublant/roles.htm#survintel > (Jan 2000).

[17]Excerpts from Cahners In-Stat Group's report, Access Requirements: the Growing Demands of Remote and Mobile Users (Report No. MD98-14MD, September 1998). Lkd "PCS Data Knowledge Site", Intel Corporation, < http://www.pcsdata.com/cahnersinstat.htm > (February 2000).

[18]"Kingdom of Tonga", Dandin Group News, < http://www.dandin.com/news.html >.

[19]Denning, 198-199.

[20]Richard Danzig, Secretary, Department of the Navy, Special Defense Department Briefing On U.S. Navy Announcement Subject: Embrace And Application Of New Technologies To Navy Destroyers (Washington, D.C.: Pentagon Briefing Room, January 6, 2000). Lkd "DD 21 Homepage", < http://dd21.crane.navy.mil/Library/library.htm >.

[21]Associated Press, U.S. Fires Laser at Satellite, October 21, 1997. Lkd "Sightings", < http://www.sightings.com/political/weapons/usfireslaser.htm >.

[22]Department of the Navy, Navy Fact File: Fleet Ballistic Missile Submarines, Lkd < http://www.chinfo.navy.mil/navpalib/factfile/ships/ship-ssbn.html >, (Dec 7, 1999).

[23]"Unmanned Aerial Vehicles", Submarine Warfare Division (CNO N87) Homepage, <http://www.chinfo.navy.mil/navpalib/cno/n87/uav.html>(Jan 2000).

[24]LCDR Pete McVety, USN, "An Unmanned Revolution," U.S. Naval Institute Proceedings 126/3, (March 2000): 90-91.

[25]Ibid., 91.

[26]"UUV Homepage", Commander, Naval Undersea Warfare Center Division Newport (NUWC DIVNPT), < http://stingray.npt.nuwc.navy.mil/ > (Oct 1999)

[27]"Flying Plug", Space and Naval Warfare Systems San Diego (SSC San Diego), < http://www.nosc.mil/robots/undersea/plug/plug.html > (Dec 1998).

[28]"SmartComm Homepage", Commander, Naval Undersea Warfare Center Division Newport (NUWC DIVNPT), < http://stingray.npt.nuwc.navy.mil/uuv/SmartComm/SMARTCOMM.htm > (August 1999).

[29]Denning, 203.

[30]Telegeography, Inc., "Telegeography, 1999", Lkd < http://www.telegeography.com/Publications/tg99_facilities.html > (1999).

[31]Cable and Wireless Global Marine, "Asia Cable Map", Lkd < http://www.cwplc.com/business/transglo/maps/asia.jpg > (1998).

[32]"Submarine Roles and Missions", Commander, Submarine Force Atlantic Fleet (COMSUBLANT) Homepage

[33]Ibid.

[34]Joint Chiefs of Staff, Joint Doctrine for Military Deception (Joint Pub 3-58) (Washington, D.C.: May 31, 1996), v.

[35]Address at the U.S. Naval Institute Annapolis Seminar and 123d Annual Meeting, Annapolis, MD, 23 April 1997.

[36]Martin Libicki, "The Mesh And The Net: Speculations on Armed Conflict In a Time of Free Silicon", Lkd McNair Papers #28, < http://www.ndu.edu/ndu/inss/macnair/mcnair28/m028ch02.html >, (March 1994).

[37]Ibid.

[38]David S. Alperts, John J. Garstka, and Frederick P. Stein. *Network Centric Warfare* - 2nd Edition . (Washington, DC: C4ISR Cooperative Research Program, Asst Sec of Defense C3I, September 1999), P.2.

[39]Libicki.

[40]Ibid.

[41]Michael Howard, The Franco-Prussian War, (London: Routledge, 1961) p43-44.

[42]Steven I. Levine, Anvil of Victory: The Communist Revolution in Manchuria 1945-1948. (New York, Columbia University Press, 1987) p 126-136.

Bibliography

Alperts, David S., Garstka, John J. and Stein, Frederick P. Network Centric Warfare - 2nd Edition. Washington, DC: C4ISR Cooperative Research Program, Asst Sec of Defense C3I, 1999.

Cable and Wireless Global Marine Homepage, Lkd < http://www.cwplc.com/ > (1998).

Commander, Submarine Force Atlantic Fleet (COMSUBLANT) Homepage, Lkd < http://www.chips.navy.mil/sublant > (2000).

Denning, Dorothy. Information Warfare and Security. Reading, MA: Addison-Wesley, 1999.

Department of the Air Force, Cornerstones of Information Warfare. (Washington, D.C.).

Howard, Michael, The Franco-Prussian War. London: Routledge, 1961.

Joint Chiefs of Staff. Joint Doctrine for Information Operations (Joint Pub 3-13). Washington, D.C., 1998.

Joint Chiefs of Staff. Joint Doctrine for Military Deception (Joint Pub 3-58). Washington, D.C., 1996.

"Flying Plug", Space and Naval Warfare Systems San Diego (SSC San Diego), Lkd < http://www.nosc.mil/robots/undersea/plug/plug.html > (Dec 1998).

Levine, Steven. Anvil of Victory: The Communist Revolution in Manchuria. New York: Columbia University Press, 1987.

Libicki, Martin. The Mesh And The Net: Speculations on Armed Conflict In a Time of Free Silicon, Lkd McNair Papers #28, < http://www.ndu.edu/ndu/inss/macnair/mcnair28/m028ch02.html >, (March 1994).

McVety, LCDR Pete, USN, "An Unmanned Revolution," U.S. Naval Institute Proceedings 126/3, March 2000.

Navy Department, Copernicus...Forward. (Washington, D.C.: June 1995).

Submarine Warfare Division (CNO N87) Homepage, <http://www.chinfo.navy.mil/navpalib/cno/n87/>

Telegeography, Inc. Homepage, Lkd < http://www.telegeography.com/ > (1999).

"UUV Homepage", Commander, Naval Undersea Warfare Center Division Newport (NUWC DIVNPT), Lkd < http://stingray.npt.nuwc.navy.mil/ > (Oct 1999)